Mejor prevenir que curar

El proceso de adaptación de la seguridad en las organizaciones frente a la evolución de las amenazas de ciberseguridad

El informe de marzo de 2016 sobre el Estado de la Seguridad que RSA e ISACA prepararon para la Conferencia de RSA (*State of Cybersecurity: Implications for 2016)* muestra claramente la rapidez con la que se ha transformado el ecosistema de actores y amenazas de seguridad durante los últimos años

MANUEL LORENZO
Especialista de la división de seguridad de EMC-RSA

Desde los primeros ataques de hackers y la expansión del *phishing*, que intentaban explotar brechas de seguridad conocidas para obtener un rédito económico a corto plazo, normalmente en el sector financiero, hemos evolucionado hacia un escenario donde se realizan campañas dirigidas por grupos cibercriminales, provenientes en su mayoría del crimen organizado (31% de los casos), que persiguen un objetivo claramente económico, no sólo en el ámbito financiero, sino en cualquier sector con información valiosa.

Además, se declara de forma abierta un tipo de ataque más sofisticado y peligroso, pero de menor afectación (13%), con origen en países o estados cuyo interés no es ya el fraude o lucro a corto plazo, sino la obtención de información privilegiada con vistas a su utilización a largo plazo. Por último, se registra un aumento de la actividad de grupos de hacktivistas (12%) cuyo objetivo no es meramente económico. sino que buscan la exposición pública de información confidencial.

Este informe constata que el robo de información supone el 41% de los casos, sobrepasando dicha motivación a aquélla meramente lucrativa en el corto plazo. Ésta última, que alcanza un 32% de los casos, se debe en su mayor parte a los ataques más tradicionales al sector financiero (*phishing*, troyanos, etc.).

Ante este cambio en el escenario de seguridad tenemos que preguntarnos hasta qué punto están nuestras organizaciones preparadas para responder a las amenazas. En la última encuesta de RSA (*RSA Cybersecurity Poverty Index,* junio 2016) sobre carencias en seguridad se resaltaron algunas relativas

La adopción de la figura del responsable de seguridad ha evolucionado de forma más rápida en los sectores históricamente más afectados por los ataques, como el financiero y el de telecomunicaciones, donde su implantación ha mejorado de manera drástica la seguridad de las organizaciones

a la capacidad de respuesta ante las nuevas amenazas. Como puntos más destacados de ese informe podemos reseñar:

• Un 67% declaran haber sufrido un incidente de seguridad que ha afectado a su actividad en el último año.

• Por segundo año consecutivo, el 75% de los encuestados considera que tiene una exposición significativa al riesgo cibernético.

• Las organizaciones que reconocen haber sufrido más incidentes de seguridad son un 65% más proclives a implementar capacidades y procedimientos avanzados de ciberseguridad.

• La mitad de los entrevistados califica su capacidad de respuesta ante los incidentes como "no definida" o "inexistente".

• Las organizaciones menos maduras continúan (erróneamente) implementando más tecnologías de prevención perimetrales como manera de evitar incidentes.

• El sector público (excluyendo Defensa) es el que declara menos capacidades de seguridad desplegadas (18%).

Desgraciadamente, la creación de un plan de detección y respuesta ante incidentes sigue teniendo como principal factor detonante haber sufrido un ataque grave que afecte al normal funcionamiento. La mentalización de una empresa después de un ataque exitoso es tal que existe una gran brecha de preparación entre las compañías que han realizado estos cambios y aquéllas que no los han considerado., También resulta interesante ver que no existe una brecha de madurez grande entre las distintas regiones (América, EMEA y Asia).

Este cambio de estrategia de seguridad es un proceso que tiene que ser liderado por una figura de peso que reorganice la seguridad desde una perspectiva global de la empresa, y que sea capaz de aportar visión y liderazgo, al tiempo que recibe la capacidad presupuestaria necesaria para poder afrontar el tránsito desde un modelo basado en la prevención hacia otro más global, donde se definan técnicas y procedimientos para detectar y responder a las nuevas amenazas. En el informe de RSA e ISACA, el 46% de los responsables de seguridad (sean estos CISOs formales u otras figuras dentro del departamento de IT) están actualmente reportando al CIO o responsable de sistemas. Sin embargo, y debido a la importancia creciente que cobra la ciberseguridad en las organizaciones cada vez son más los CISOs que reportan de forma directa al director ejecutivo (o CEO), con un 14% de los casos. En muchas de las organizaciones más concienciadas acerca de la importancia de la ciberseguridad, la figura del CISO forma parte, como un directivo más, del consejo de administración (un 8% de los casos).

La adopción de la figura del responsable de seguridad ha evolucionado de forma más rápida en los sectores que históricamente más afectados por los ataques, como el financiero y el de telecomunicaciones, donde su implantación ha mejorado de manera drástica la seguridad de las organizaciones. Sería conveniente que este cambio de mentalidad se produjera de manera equivalente en los demás sectores, incluyendo por supuesto el sector público, adecuando responsables y departamentos de seguridad dentro de las organizaciones ministeriales para responder a las nuevas amenazas que se nos presentan.

Estas encuestas sobre la adecuación de la seguridad en las organizaciones refrendan los datos de otra previa de RSA sobre la preparación técnica y el balance de la inversión en seguridad (*RSA Thread Detection Effectiveness Survey,* abril 2016) donde sólo un 24% de los entrevistados se sentían satisfechos con su habilidad actual para detectar e investigar amenazas de seguridad. En esta encuesta previa, las empresas declaraban que su prioridad de inversión seguía estando centrada en la prevención clásica (AV, FW, IDS, etc.) con un 47% del presupuesto, focalizada en implementar infraestructuras perimetrales (tecnologías que contaban con un 88% de adopción) y dejando de lado otras fuentes de información que proporcionan más capacidad de detección de los ataques exitosos (un 59% de agentes en el puesto de trabajo y un 49% en paquetes/flujos de red).

Sin embargo, aquellas empresas

que han evolucionado su estrategia de seguridad muestran un balance más equilibrado entre las inversiones, incrementando el presupuesto para las tecnologías de detección de ataques en el puesto final y en la red, para la definición de procesos de respuesta ante incidentes y para la adecuación del equipo de personas a cargo de la detección y respuesta ante los incidentes de seguridad.

Se constata también que las empresas que han implementado tecnologías avanzadas de detección (comportamiento, puesto de trabajo, paquetes/flujos de red, etc.) declaran un valor mucho mayor para la seguridad de esas fuentes con respecto a las tradicionales. Estas son las áreas donde fabricantes como RSA centramos nuestros esfuerzos, con el fin de ofrecer tecnologías que capaces de analizar el comportamiento de sistemas y personas tanto en el puesto final y en los servidores como en los flujos de datos, detectando actividades sospechosas de ser maliciosas. En estas fuentes de información es donde realmente se pueden detectar el software malicioso las actividades de ex filtración de datos, disponiendo de una visión completa de lo que ha realmente ha pasado en los sistemas tras un incidente de seguridad. ✱

REFERENCIAS

ISACA State of Cybersecurity, Implication for 2016: http://www.isaca.org/cyber/pages/state-of-cybersecurity-implications-for-2016.aspx

2016 RSA Cybersecurity Poverty Index: https://www.rsa.com/en-us/perspectives/industry/cyber-security-poverty-index

RSA Threat Detection Effectiveness Survey: https://www.rsa.com/en-us/perspectives/resources/threat-detection-effectiveness